Руководство по генерации сертификатов OpenSSL

Выпуск

ROBIN RPA Team

дек. 25, 2020

Содержание:


ROBIN
ROBOTIC INTELLIGENCE

Глава 1

Самостоятельная генерация сертификата с использованием OpenSSL

1.1 Подготовка

1. Заходим на http://slproweb.com/products/Win32OpenSSL.html
2. Выбираем версию OpenSSL для загрузки, битность - соответствующая битности на компьютере.
3. Загружаем OpenSSL на компьютер и устанавливаем его. В процессе установки указываем и запоминаем путь до OpenSSL.

1.2 Генерация сертификата

Пусть путь до OpenSSL будет у нас по умолчанию - `C:\Program Files\OpenSSL-Win64\`

Если у вас другой путь - указывайте его.

Открываем консоль от имени администратора и выполняем в ней следующие шаги:

1. Перемещаемся в директорию с OpenSSL

```
cd C:\"Program Files"\OpenSSL-Win64\bin\
```

2. Генерируем приватный ключ длиной в 2048 бит и сохраняем его в файл `C:\cert\private.key`

```
openssl genrsa -des3 -out C:\cert\private.key 2048
```

При генерации приватного ключа OpenSSL попросит создать пароль для приватного ключа. Вводим его и запоминаем - он в дальнейшем нам ещё понадобится.

3. Создаём «запрос» на получение CSR сертификата.

```
openssl req -new -key C:\cert\private.key -out C:\cert\certificate_csr.csr
```

OpenSSL попросит ввести нас пароль от нашего приватного ключа (который мы создавали на втором шаге). Вводим его и нажимаем Enter. Обратите внимание - пароль не будет отображаться в консоли (скрытый ввод), поэтому вводим его внимательно.

Дальше OpenSSL попросит у нас ввести информацию о сертификате, как показано ниже:

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:RU  # Двузначный код страны, RU для России
State or Province Name (full name) [Some-State]:Moscow  # Город, в котором вы находитесь
Locality Name (eg, city) []:city  # Можно оставить пустым или вписать city
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Robin  # Название вашей организации
Organizational Unit Name (eg, section) []:section  # Название подразделения
Common Name (e.g. server FQDN or YOUR name) []:Robin  # На кого регистрируют этот сертификат
Email Address []:test@it.ru  # Электронная почта компании

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:Qwerty123  # Дополнительный пароль
An optional company name []:Robin  # Дополнительное имя компании
```

После ввода всей информации у нас будет сгенерирован CSR-сертификат, расположенный в `C:\cert\certificate_csr.csr`.

4. Дальше у нас есть два пути развития событий.

Мы можем либо отдать сертификат на подписание в сертификационный центр, либо подписать его самостоятельно.

4.1. В случае, если мы подписываем сертификат самостоятельно - мы генерируем публичный PEM-сертификат из того, что у нас есть, сроком на год (365 дней, число можно изменить), следующей командой.

```
openssl x509 -req -days 365 -in c:\cert\certificate_csr.csr -signkey c:\cert\private.key -out␣
↪c:\cert\certificate_pem.pem
```

OpenSSL запросит пароль от приватного ключа, вводим его.

Если мы подписали сертификат самостоятельно - выполняем преобразование PEM в CER:

```
openssl x509 -outform DER -in c:\cert\certificate_pem.pem -out c:\cert\certificate_cer.cer
```

4.2. В случае, если мы подписываем с помощью сертификационного центра, мы отправляем CSR-файл - запрос на подпись сертификата - в сертификационный центр. Выбираем шаблон сертификата Web Server. Обратно нам должен вернуться уже подписанный CER-сертификат.

5. Затем мы преобразуем CER в CRT - формат сертификата, понятный хранилищу сертификатов.

```
openssl x509 -inform DER -in c:\cert\certificate_cer.cer -out c:\cert\certificate_crt.crt
```

6. Создаём PFX-контейнер для сертификата. PFX-контейнер нужен для того, чтобы свободно переносить сертификат вместе с приватным ключом на флешке или любом другом носителе.

```
openssl pkcs12 -export -inkey C:\cert\private.key -in C:\cert\certificate_crt.crt -out␣
↪C:\cert\certificate.pfx
```

Или p12-контейнер

```
openssl pkcs12 -export -inkey C:\cert\private.key -in C:\cert\certificate_crt.crt -out␣
↪C:\cert\certificate.p12
```

OpenSSL попросит ввести пароль от приватного ключа и создать пароль для экспорта контейнера.